EXHIBIT 1

Freedom to Tinker

… is your freedom to understand, discuss, repair, and modify the technological devices you own.

« MediaMax Permanently Installs and Runs Unwanted Software, Even If User Declines EULA
The DMCA Should Not Protect Spyware »

Sony, First4 Knew About Rootkit Issue in Advance

Wednesday November 30, 2005 by Ed Felten

Security vendor F-Secure contacted SonyBMG and First4Internet about the companies' rootkit software on October 4 — about four weeks before the issue became public — according to a Business Week story by Steve Hamm.

Here's the key part of the article's chronology:

> Nevertheless, Sony BMG asked First4Internet to investigate. Both Sony BMG and F-Secure say that it was on Oct. 17 that F-Secure first spelled out the full scope of the problem to Sony. The security company's report on the matter, sent that day to First4Internet and Sony BMG, confirmed there was a rootkit in XCP and warned that it made it possible for hackers to hide viruses and protect them from antivirus software products. F-Secure referred to XCP as a "major security risk," according to a copy of the e-mail supplied to BusinessWeek Online by F-Secure.
>
> Sony BMG says it asked the two software companies to investigate and find a solution to the problem. "From the moment our people learned that F-Secure had identified a potential problem we contacted our vendor and in no uncertain terms told them you have to get with F-Secure and find out what needs to be done about it," says Daniel Mandil, Sony BMG's general counsel.
>
> BOGGED DOWN. What happened next is in dispute. F-Secure had a conference call with executives of First4Internet on Oct. 20. It says First4Internet argued that there was no real problem because only a few people knew of the vulnerability XCP created, and said an update of the XCP software, due out early next year, would fix the problem on all future CDs.

At first glance, this looks like a standard story about disclosure of a security vulnerability: vendor ships insecure product; researchers report flaw privately; vendor drags feet; researchers report flaw publicly; problem fixed right away. The story features the classic vendor error of seeing insecurity as a public relations problem rather than a customer safety issue: "there was no real problem because only a few people knew of the vulnerability".

But if we read this as just another vulnerability disclosure, we're missing an important part of the story. In the usual case, the security vulnerability exists by mistake — the vendor doesn't know the vulnerability exists until somebody points it out. Here, the rootkit-like functionality was not a mistake but a *deliberate design decision* by the vendor.

Which suggests the question of what exactly F-Secure was disclosing to Sony and First4Internet, or more precisely what it was disclosing that they didn't already know. They must have known about the rootkit already — it was a design decision they had made — and if they had any kind of clue they would have known that users would hate having a rootkit on their machines, especially one that provided an obvious hiding place for other malware. As far as I can see, the only new information F-Secure would have disclosed was that F-Secure planned to treat the program as malware.

It's interesting, too, that other makers of anti-malware tools didn't seem to notice the problem until Mark Russinovich's public disclosure. As of mid-September, this malware had been on the market for months and presumably had been installed on hundreds of thousands of computers, but still none of the anti-malware vendors had discovered it. (According to the Business Week article, F-Secure didn't discover the malware itself, but learned of it on Sept. 30 from John Guarino, a computer technician in New York who had discovered it on several clients' computers.) It's not a good

sign that all of the major anti-malware vendors missed it for so long.

Finally, we have to consider the possibility that Sony and First4Internet understood the significance of the rootkit, but simply felt that copy protection trumped users' security. First4Internet probably held that view — otherwise it's hard to explain their design decision to deploy rootkit functionality — and Sony may well have held it too. We know already that entertainment companies want to redesign our computers in the hope (which is ultimately futile) of stopping copying. From there, it's not so large a step to decide that users' security simply must be sacrificed on the altar of copy protection.

What did SonyBMG know, and when did it know it? We'll find out more as the lawsuits proceed.

This entry was posted on Wednesday November 30, 2005 at 6:41 am and is filed under Security, DRM, Privacy, CD Copy Protection. You can follow any responses to this entry through the RSS 2.0 feed. You can leave a response, or trackback from your own site.

20 Responses to "Sony, First4 Knew About Rootkit Issue in Advance"

1. *dr2chase* Says:
   November 30th, 2005 at 8:40 am

   I think "on the altar of copy protection" should be rephrased "to the lucky rabbit's foot of copy protection". Lots of ordinary non-piratical users either use Macs, or Linux, or disable autorun with TweakUI. Real live pirates might employ more arcane tricks liking holding down the shift key, optically blocking the data area (tape or marker) or, perish the thought, actually ripping from the audio signal (I've got vinyl I've converted to MP3; it's not rocket science, and the results are not bad even from aged records on a garbage-sale turntable).

   My theory ("watch what they do, not what they say") is that this is not about copy protection; it is instead about making computers an unacceptable platform for audio and video. If they cannot control it, then they'll make it unusable instead. The more interesting question is whose side the anti-spyware and anti-virus companies are on? They're not normally thought of as an anti-spyware/virus company, but I've had pretty good luck with Apple so far.

2. *jordan vance* Says:
   November 30th, 2005 at 8:49 am

   It sounds, or rather looks, to me that Sony had no clue according to that article. It says nothing of SonyBMG being on the first conference call (although my guess is that they had legal beagles who were on that call). If that's the case, did F-Secure go back to Sony and say that F4I was being harmful? It'll be interesting to see how this all plays out. F4I won't come out looking pretty, but I don't know whether any mud will get smeared on Sony.

3. *The PC Doctor* Says:
   November 30th, 2005 at 9:25 am

   Sony knew about the rootkit before the storm!

   BusinessWeek is reporting that Sony BMG knew about the rootkit nearly a month before Mark Russinovich broke the news on Oct 31st.
   According to the article, F-Secure informed them on Oct 4th after a PC tech reported the rootkit to them on …

4. *wouldUbelieve* Says:
   November 30th, 2005 at 9:52 am

"Here, the rootkit-like functionality was not a mistake but a deliberate design decision by the vendor." Amen. When I first read the BusinessWeek article I was stunned by the viewpoint the F-Secure was in some way telling Sony and F4I something they did not already know. Does F-Secure contact every malware writer in the same way? Of course not…so there is still more to be uncovered in this story.

5. *zapkitty* Says:
November 30th, 2005 at 10:14 am

jordan vance wrote:

"F4I won't come out looking pretty, but I don't know whether any mud will get smeared on Sony"

You mean any more than Sony's multitude of willfully deceitful responses to the exposure of their malware has already smeared their own name?

"We didn't know…" I bet a few Sony execs are whistling in the dark to just that tune right now.

Unfortunately that "we didn't know" defense is not only moot given Sony's responsibilities in commissioning and distributing the malware… that defense is already shot dead and buried by one word: Sunncomm.

Sony has demonstrably made a habit of commissioning and distributing malware for their personal gain, and no amount of whistling in the dark can make that fact go away.

6. *Wayne* Says:
November 30th, 2005 at 11:05 am

From the Business Week story, it seems that Sony BMG asked First 4 Internet and F-Secure to get together and fix the problem. It seems to me that F-Secure's job is to identify the security problem and come up with countermeasures in its own security software, but not to fix XCP. Does this simply indicate Sony's misunderstanding of F-Secure's role (as they seem to have misunderstood everything in this affair), or a desire to palm the problem off on the "vendors," or all of the above?

7. *Mike W* Says:
November 30th, 2005 at 11:47 am

"Here, the rootkit-like functionality was not a mistake but a deliberate design decision by the vendor."

To me, that's the most damning fact. It was no accident that it had rootkit functionality. Its no accident that the software was hidden from the user. Its no accident (IMO that its nearly impossible to remove.

Honestly, if Sony BMG/F4I believes the user has agreed to an EULA allowing them to install the software, there is absolutely no reason for the softwre to be hidden from that same user. If you actually believe you've been invited in an unlocked front door, you wouldn't break in through the back door.

8. *Daruku* Says:
November 30th, 2005 at 11:54 pm

First of all Sony has a scape goat, First4Internet. Sony, however would be stupid to use them as a scape goat since that invites the view that Sony is stupid or ignorant, meaning that Sony didn't know or care what was going on. Thus, inviting the view Sony's other products are stupid. Stupid cd players. Stupid TVs. Stupid computers. Thinking about it Sony really is stupid to have tried this in the first place.

9. *Havoc* Says:
December 1st, 2005 at 12:01 am

"If you actually believe you've been invited in an unlocked front door, you wouldn't break in through the back

door.”

Couldnt be said better

10. *Anonymous* Says:
December 1st, 2005 at 1:09 am

Actually SunnComm insiders are claiming that SunnComm knew about First4Internet’s rootkit problem months ago, but wouldn’t tell Sony.

“sahd3g, You are correct, there was knowledge of SEVERE problems with First4 months back, BUT it would not be the best in regards to business relationships telling one of your best clients “Hey dummy - that other stuff you are evaluating has LOTS of problems”. Besides, anyone would feel that it was certainly NOT unbiased. MediaMax has done a VERY GOOD job at selling, look at the size of their competitors, and this little company is making big headway. IMHO, I feel the “BMG” side of Sony will communicate very well for us.
I EXPECT very good results with Kevin, he will hit the ground running.”

http://www.investorshub.com/boards/read_msg.asp?message_id=8476531

11. *Anon* Says:
December 1st, 2005 at 10:14 pm

Mr. Felten,

I find it interesting that you think that:

“[Sony and F4I] must have known about the rootkit already — it was a design decision they had made — and if they had any kind of clue they would have known that users would hate having a rootkit on their machines, especially one that provided an obvious hiding place for other malware.”

Certainly F4I had to have known that XCP used a rootkit, and Sony BMG probably should have known, and if they didnt know, they were certainly negligent in not knowing. However, I wish to raise the following question: Did Sony and F4I understand that the rootkit would not only cloak XCP’s files, but also any file on the system with the preifx “sys”?

I’m not trying to defend Sony BMG or F4I, but I wish to point out that Mark Russinovich’s initial research also revealed that XCP was very poorly coded in how it addressed memory ; in other words, when comes to brains, the F4I guys may have been more than a few bits short of a byte. They may not have been aware that their cloak was not a specific but an abstract cloak and could be used to hide virtually anything properly named. In this version of events, Sony, then, would have been neglient in not discovering this before releasing XCP-laced CDs.

Furthermore, F-Secure’s communications on October 17th may have been the first time that F4I learned that XCP could cloak “third-party” malware. Certainly they were negligent in not knowing this beforehand, and their subsequent idea that they could just leave the security vulnerability in the wild until a patch and hope for the best was about as stupid as stupid can get.

I have suggested this version of events solely because I find it difficult to believe that F4I and Sony intentionally designed a cloak for any malware but their own.

12. *Goodwin* Says:
December 2nd, 2005 at 6:20 am

“If you actually believe you’ve been invited in an unlocked front door, you wouldn’t break in through the back door. ”

or

If you actually believe you've been invited in an unlocked front door, why do you skulk about in the darkness with a torch

13. *Savon duJour* Says:
December 2nd, 2005 at 7:17 am

A point - I was sailing around the world and noticed that the exact same CD from the same company was double the price in England than in Portugal, than in Brazil they were about 1/10th price of England. If CDs are priced for the market and not by intrinsic value then Sony is protecting its profits and not its product. I don't think that one is defensible in law because it would involve global laws and marketing, however I would think that Sony meant to use its DRM globally.

I have a bookshop. Publishers like books being loaned out by purchasers, we have public libraries where you can borrow them free. It stimulates the market. If you like an author, you don't want just old copies you have to give back, you want to own the latest book by your fave writer and then with luck you will lend it out and spread the love and increase the market.

14. *Anon* Says:
December 2nd, 2005 at 4:00 pm

To follow up on my previous comments [Comment #11], where I stated that I found it difficult to believe that Sony BMG and F4I purposefully designed an abstract cloak rather than one that would just apply to the XCP software:

Further evidence that Sony BMG and F4I [and possibly SunnComm as well] may well have been unaware of the potential offered by abstract programming decisions comes, of course, from the now infamous Javascript involved in the now-defunct XCP and MediaMax uninstallation process.

The reader will recall that both programs were intended be the conduit through which Sony would send you the uninstaller if you jumped through enough e-mail hoops. In other words, the link they would finally provide you with would invoke the program and a certain "download" clause to provide the software. Of course, what the programmers didn't realize was that ANYBODY could invoke this clause, causing you to download just about ANYTHING.

Finally, I wish to suggest a gag christmas gift for Sony executives: why doesnt somebody send them a poster of an abstract work by Picasso?

15. *Jonathan C.* Says:
December 2nd, 2005 at 11:07 pm

If you truly believe that Sony et al did not know of this …have I got a bridge for you. It strikes me that if I was producing a cd or dvd, I would be damn sure I knew about every piece of info that was on it. It does seem to explain why my Studio 123 software no longer works ….

16. *Anonymous* Says:
December 3rd, 2005 at 9:03 am

Very interesting post about SunnComm on the boycottsony blog

http://www.boycottsony.us/?p=82

==========

December 3rd, 2005 at 10:38 am
I think you will find the following post "explosive" in the corruption inside SunnComm. In the above blog you give a link to a request by SunnComm for help in public forums:

http://www.boingboing.net/2005/11/28/programmers_on_sonys.html

If you go to that link you will find the requester name as Ken Fagan and the date 01-may-2001.

SunnComm has a feature on its web site called "Ask The President". This is supposed to be an informal Q & A where SunnComm's President Peter Jacobs answers questions from investors and others (those who follow it closely, know it is used for blatant pumping of the company stock with inuendo on deals that never materialize etc.). Most old Q&As have been removed, but with the benefit of Wayback Machine, we can see some Q&As from 2002.

http://web.archive.org/web/20021018095120/http://www.sunncomm.com/asktheprez/asktheprez.asp

Take a look at the 2nd last Q&A at that link. As you can see it is an almost incredulous endorsement of SunnComm by Microsoft (Has Microsoft ever said such glowing statements about any other company, never mind a penny stock?). The statements were made by Ken Cavelon, Engagement Manager, Microsoft Services for ISV Partners. But when that Q&A first appeared on AskThePrez, the name was not Ken Cavelon, but Ken Fagan, using the same title.

When the original, with Ken Fagan as the author appeared, some astute investors remembered the name Ken Fagan from an SEC filing by SunnComm. It appears that Ken Fagan (at the time employed by Microsoft) was given a contract by SunnComm to help sell SunnComm products to major software vendors (including Microsoft).

"Consulting Agreement

On August 18, 2000, we entered into a Consulting Agreement with Kenneth W. Fagan, whereby Mr. Fagan agreed to act as Special Advisor to the board of directors and a corporate consultant. The term of the agreement is one (1) year. We paid Mr. Fagan an initial payment of $2,500 upon the execution of the agreement. We also agreed to pay Mr. Fagan $2,000 per month during the term, along with 250,000 restricted shares of the Company's common stock upon the execution of the agreement. Mr. Fagan has a right to earn up to 750,000 options at an exercise price of .22as follows: 34% to be issued upon the signing of three (3) licensing agreements with major software vendors ($25,000000 + in revenues) delivered by Mr. Fagan, and 66% to be issued upon the signing of a
licensing agreement with a large independent software vendor (such as Oracle, Microsoft, etc.) delivered by Mr. Fagan. See Exhibit 10.17 for a copy of the Consulting Agreement."

http://www.sec.gov/Archives/edgar/data/1122973/000108671501000100/0001086715-01-000100-0001.txt

They also remembered that Ken Fagan used post on the Raging Bull board for SunnComm using the alias Illuvetar. Unfortunately RB has removed all old posts, but this is an example of one of Illuvetar's posts (I am including the link - not working now obviously - but available to the SEC/FBI should they wish to demand RB produce the original):

"BUY BUY BUY!!! This could be a $30B Company (that's right, a B!) in a matter of months!!!"

http://ragingbull.lycos.com/mboard/boards.cgi?board=SUNX&read=533

In several posts around that time, Illuvetar (his profile gave his e-mail as kenfagan@microsoft.com) identified himself as a Microsoft employee and he used his employment status with Microsoft to add credibility to his recommendations on SunnComm (he never mentioned his contract with SunnComm though). He also was (and still is I believe) a Microsoft employee when he entered that contract with SunnComm, which represented a huge conflict of interests.

After the endorsement of SunnComm by Microsoft (via Ken Fagan) appeared on AskThePrez, posters started questioning the whole integrity of what was written since they were reminded by the astute posters of Ken

Fagan's association with SunnComm. One poster wrote some e-mails to Ken Fagan and although no satisfactory explanation was given, Fagan revealed that he had decided to change his name to Ken Cavallan.

(Note: when SunnComm first changed the name showing in the AskThePrez Q&A from Fagan, they originally mispelled it as Cavelon - see link I gave above. It took 2 further attempts to get it right. See this subsequent Wayback Machine snapshot where they have finally got it right:

http://web.archive.org/web/20030113222058/http://www.sunncomm.com/asktheprez/asktheprez.asp)

Although many suspected the name change might have a lot to do with the fact that the whole event as detailed above was submitted to the SEC, Ken Fagan (now Cavallan) in a Raging Bull post gave this as the reason.

"And yes, I did change my name on August 1st, 2002. Wouldn't you if your name was FAGan and you could? (My kids were sick of getting teased and I was sick of re-living it! So we took my mother's maiden name!)"

http://www.ragingbull.lycos.com/mboard/boards.cgi?board=STEH&read=35524

So when Fagan asked for help on May 1st 2001, not only was he under contract to SunnComm, but he was also employed by Microsoft and was asking questions concerning Windows Media DRM, a Microsoft product.

These are some posts of Illuvetar (recorded by some of the astute investors) that show his blatant pumping of SunnComm - without acknowledging his relationship with the company:

http://ragingbull.lycos.com/mboard/boards.cgi?board=STEH&read=38979
http://ragingbull.lycos.com/mboard/boards.cgi?board=STEH&read=39046
http://ragingbull.lycos.com/mboard/boards.cgi?board=STEH&read=39053

Not only did Fagan pump SunnComm without disclosing his relationship with the company, but it also appears he was deliberately misleading. In this post he tries to give the impression he doesn't know the CEO, Peter Jacobs.

http://ragingbull.lycos.com/mboard/boards.cgi?board=STEH&read=39039

That was made just 2 weeks before his contract commenced and he doesn't know the CEO. Yet in his 21 Jan 2003 confession he tells us:

"Actually, the relationship at its very beginnings(beyond that of just licensee), goes back to August 18th, 2000 when I joined the Board of Advisors of SunnComm, Inc. (And actually I knew Peter before that, it is the roots of our long standing relationship that have brought these two companies together.) "

http://www.ragingbull.lycos.com/mboard/boards.cgi?board=STEH&read=35524

You can make your own mind up as to what type of company SunnComm is.

Don't forget that December 14th is the 5th anniversary of when SunnComm issued the infamous PR that described a $20M deal with a MAJOR PACIFIC RIM CD MANUFACTURER.

"SunnComm Inks $20+ Million Copy Protection Deal With Major Pacific Rim CD Manufacturer

PHOENIX–(BUSINESS WIRE)–Dec. 14, 2000–SunnComm Inc. finalized a seven-year (minimum) $20+ million dollar contract with Will-Shown Technology Co., LTD Taipei, Taiwan to provide audio copy protection for Will-Shown Manufacturing of audio compact discs……."

http://cdmediaworld.com/hardware/cdrom/news/0012/sunncomm_cd_protect.shtml

That deal was a complete fabrication. There was no such company as Will-Shown. You can read about it here (it is the 3rd complaint, so search on Will-Shown to get to the start).

http://www.our-street.com/SEC-SunnComm4.htm

17. *Anonymous* Says:
December 4th, 2005 at 6:21 pm

In response to posts #11 and #13:

Whether Sony originally knew about it or not, their lack of action in quickly and correctly rectifying the situation indeminfies every party involved. Had Sony not originally known about the rootkit, and had Sony not wanted it there in the first place, etc. then when the news was broken to the public, Sony would have provided a much simpler path to removal of the software from affected computers along with a public apology and ensured the removal of all CDs carrying the program.

As of today - weeks later - no such moves have been made. The current method of removal is not only a pain in the rear, it opens the user's computer with more vulnerabilities when the uninstaller need not be as 'complex' as it is. In addition, many stores nationwide are still stocking the affected CDs and many are unaware of a recall by Sony.

Due to this evidence it's become quite difficult to believe Sony is as much a victim of bad vendors as the consumer is.

Being a former music pirate, there was a time when I attempted to go straight. However, when the first songs I bought online werent able to play in the mp3 player in my truck because there's no way to transfer the license and now this mess with Sony…it's no wonder piracy is on the rise.

The strong-arm tactics used by the RIAA and assoc. instead of giving the consumer what is desired is hardly the way for the RIAA to put an end to piracy. Had the RIAA altered their marketing methods to what the consumers want (lets face it, who wants to pay $15-20 for a CD with one or two good songs vs paying $6 for a single vs downloading online for free) perhaps there wouldnt be an issue.

Many pirates remain pirates because of the limitations put on what they've purchased and therefore believe they should have the right to do with as they please and because the prices for CDs have remained exorbitant while the selection of music on said CD has become one or two good songs and the other 10 to 15 are fluff.

18. *Goingmad* Says:
December 5th, 2005 at 8:26 am

We see all this stuff about lawsuits, but how does that solve anything. These rich companies will simply pull the money out of the cushions of their couch, pay, and continue abusing people. The only way to make the corporations behave is to send the people who make the decisions to jail when they do this kind of stuff. If some high-school students did this, they would lock them up and throw away the key, but when a corporation does it they just get a little percent of thier money taken away? That ain't right! They need some criminal prosecution, not just civil suits.

19. *The Prodigal Sheep* Says:
December 6th, 2005 at 8:57 pm

When corporations rule the Earth

Evidence mounts that Sony BMG knew that their new XCP copy protection scheme posed a security risk to consumers before the issue went public, but went ahead with it anyway… Or, as Ed Felten puts it: We know already that…

Leave a Reply

Name

Mail (will not be published)

Website

Submit Comment

Powered by WordPress.
Entries (RSS) | Comments (RSS).